

REMARKS

In light of the above amendments and following remarks, reconsideration and allowance of this application are respectfully requested.

At paragraphs 2-4 of the outstanding Office Action of December 31, 2003, the Examiner has rejected claims 1, 6 and 13 under 35 U.S.C. § 102(e) as being anticipated by Sasaki et al. (U.S. Patent No. 6,378,071). Applicants respectfully traverse the rejection.

The portions of Sasaki described by the Examiner teach that “the reading unit 6 receives a fixed length of the encrypted data from the file and generates a block of decrypted data of the same size by performing decryption.” Applicants submit that merely receiving encrypted data, and decrypting the data does not meet the claim limitation. As amended, independent claims 1, 8 and 13 recite that the size of a processing block having a data block length of a whole multiple of a predetermined data length of an encryption block is defined. Thereafter predetermined processing is performed on the data in units of the predetermined processing block length. The processing block length is therefore not determined simply as a function of the information to be decrypted, but is, rather, predefined as a multiple of the size of the encryption block. In accordance with the claimed invention, the predetermined processing block therefore may comprise multiples of the encrypted block, while in the Sasaki reference, only an identical sized processing result is allowed. Because the Sasaki reference fails to predefine the processing block size, applicants submit that the Sasaki reference fails to depict the invention as set forth in independent claims 1, 8 and 13. Applicants therefore, respectfully request that the rejection of these claims under 35 U.S.C. § 102(e) be

withdrawn.

At paragraphs 6-17 of the outstanding Office Action, the Examiner has rejected claims 2-3, 14-15 and 18 under 35 U.S.C. § 103(a) as being unpatentable over Sasaki et al. in view of Bellovin et al. (U.S. Patent No. 5,241,599).

Regarding claims 2 and 14, at paragraph 7 of the outstanding Office Action, the Examiner has indicated that Sasaki fails to teach the inserting of data into the processing block in order to adjust the data length so that it becomes a whole number multiple of the predetermined length. The Examiner then relies on Bellovin to teach the insertion of data in order to meet predetermined length of a block. The Examiner concludes that at the time the invention was made it would have been obvious for a person of ordinary skill in the art to utilize Bellovin's method of inserting data because it offers the advantage and helps prevent partition attacks against encryption keys.

Applicants respectfully disagree with the Examiner's combination of these references. As noted above, Sasaki et al. merely describes the conversion of an encryption block to a decrypted information, always containing the same amount of information. Because there is no predetermined size of the processing block, and thus all encrypted data is processed, there will never be a need in Sasaki et al. to add data to increase the size of the processing block. Indeed, because the size of the processing block is simply defined by the amount of encryption data utilized, there will never be a situation in Sasaki et al. where data will be needed to be added to a processing block for it to become a whole number multiple of a predefined predetermined length. Therefore,

applicants submit that the combination of references relied upon by the Examiner fails to depict the invention as set forth in claims 2 and 14. Additionally, each of these claims depends from one of allowable independent claims 1 and 13, and are therefore allowable for this additional reason.

The remaining claims 3, 15 and 18 similarly depend from one of allowable independent claims 1 and 13 and are therefore allowable for this reason, and additionally as presented independently patentable combinations in and of their own right. Applicants, therefore, respectfully request that the rejection of these claims under 35 U.S.C. § 103(a) be withdrawn.

The remaining claims 4-7, 8-12 and 17 are rejected by the Examiner under 35 U.S.C. § 103(a) over the combination of Sasaki et al. in view of Bellovin, and further in view of various additional references. However, applicants submit that none of these additional references were the defects of Sasaki et al., that namely the reference fails to depict the predefining of a processing length as a multiple of an encryption data length. Therefore, applicants respectfully submit that these claims are allowable as depending for allowable base claim, and further is presenting independently patentable combinations in and of their own right. Applicants therefore respectfully request that the rejection of these claims under 35 U.S.C. § 103(a) similarly be withdrawn.

CONCLUSION

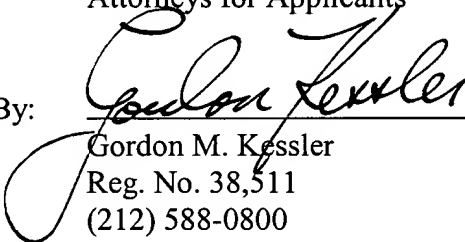
Applicants have made a diligent effort to place claims 1-18 in condition for allowance, and notice to this effect is earnestly solicited. If the Examiner is unable to issue a Notice of Allowance regarding these claims, the Examiner is requested to contact the undersigned attorney in order to discuss any further outstanding issues.

Early and favorable consideration are respectfully requested.

Respectfully submitted,

FROMMER LAWRENCE & HAUG LLP
Attorneys for Applicants

By:


Gordon M. Kessler
Reg. No. 38,511
(212) 588-0800